On Finite Monoids Having Only Trivial Subgroups

M. P. Schützenberger

An alternative definition is given for a family of subsets of a free monoid that has been considered by Trahtenbrot and by McNaughton.

I. INTRODUCTION

Let $X^*$ be the free monoid generated by a fixed set $X$ and let $Q$ be the least family of subsets of $X^*$ that satisfies the following conditions (K1) and (K2):

(K1). $X^* \subseteq Q$; $\{e\} \subseteq Q$ ($e$ is the neutral element of $X^*$); $X' \subseteq Q$ for any $X' \subseteq X$.

(K2). If $A_1$ and $A_2$ belong to $Q$, then $A_1 \cup A_2$, $A_1 \setminus A_2 (= \{f \in A_1 : f \notin A_2\})$, and $A_1 \cdot A_2 (= \{ff' \in X^* : f \in A_1 ; f' \in A_2\})$ belong to $Q$.

With different notations, $Q$ has been studied in Trahtenbrot (1958) and, within a wider context, in McNaughton (1960). According to Eggan (1963), $Q$ contains, for suitable $X$, sets of arbitrarily large star-height (cf. Section IV below).

For each natural number $n$, let $F(n)$ denote the family of all epi-morphisms $\gamma$ of $X^*$ such that $\text{Card } \gamma X^* \leq n$ and that $\gamma X^*$ has only trivial subgroups (i.e., $\gamma f^n = \gamma f^{n+1}$ for all $f \in X^*$, cf. Miller and Clifford (1956)).

**Main Property.** $Q$ is identical with the union $Q'$ over all $n$ of the families

$$Q'(n) = \{A \subseteq X^* : \gamma^{-1} \gamma A = A ; \gamma \in \Gamma(n)\}$$

$$= \{\gamma^{-1}M' : M' \subseteq \gamma X^* ; \gamma \in \Gamma(n)\}.$$  

As an application, if $A, A' \subseteq X^*$ are such that for at least one triple $f, f', f'' \in X^*$, both \{\small $n \in \mathbb{N} : ff'' f'' \subseteq A$\} and \{\small $n \in \mathbb{N} : ff'' f'' \subseteq A'$\} are infinite sets of integers, we can conclude that no $B \subseteq Q$ satisfies $A \subseteq B$ and $A' \subseteq X^* \setminus B$. 

190
II. VERIFICATION OF $Q \subset Q'$

The next two remarks are reproduced from Petrone and Schützenberger (1963) for the sake of completeness.

REMARK 1. $Q'$ satisfies (K1).

Verification. Let the monoid $M = \{e', x', 0\}$ and the map $\gamma : X^* \to M$ be defined as follows: $\gamma e = e' = e'^2$; for each $x \in X'$, $\gamma x = x' = e'x' = x'e'$; for each $f \in X^* \setminus \{e\} \cup X'$, $\gamma f = 0 = e'0 = 0e' = x'^2 = x'0 = 0x' = 0^2$.

It is clear that $\gamma \in \Gamma(3)$ and, since $X^* = \gamma^{-1}M; \{e\} = \gamma^{-1}e'$; $X' = \gamma^{-1}x'$, the remark is verified.

REMARK 2. $Q'$ satisfies (K2).

Verification. For $j = 1, 2$ let $\gamma_j : X^* \to M_j$ and $M'_j \subset M_j$ satisfy $\gamma_j \in \Gamma(n_j)$ and $A_j = \gamma_j^{-1}M'_j$. We consider the family $R$ of all sets of pairs $(m_1, m_2) \in M_1 \times M_2$ and for $m_1 \in M_1$, $m_2 \in M_2$, $r = \{(m_1i, m_2i) : i \in I_r\}$, we let $m_r = \{(m_1m_1i, m_2m_2i) : i \in I_r\}$ and $rm_2 = \{(m_1i, m_2, m_2) : i \in I_r\}$. Finally, letting $\bar{M}$ denote the direct product of sets $M_1 \times R \times M_2$, we define an associative product on $\bar{M}$ and an epimorphism $\gamma$ of $X^*$ onto a subset $M$ of $\bar{M}$ by setting for all $(m_1, r, m_2)$, $(m_1', r', m_2') \in \bar{M}$ and $f \in X^*$:

$$\gamma f = (\gamma f, \{\gamma f', \gamma f''\} : f, f' \in X^*; f' f'' = f), \gamma_2 f).$$

It is clear that $A_1 \cup A_2, A_1 \setminus A_2$ and $A_1 \cdot A_2$ are images by $\gamma^{-1}$ of suitable subsets of $M$. Since $\bar{M}$ is finite, the remark will follow from the fact that any subgroup $G = \{(m_1i, r_i, m_2i) : i \in I_G\}$ of $\bar{M}$ is isomorphic to a direct product $G_1 \times R \times G_2$. Since $G$ is finite, the remark will follow from the fact that any subgroup $G = \{(m_1i, r_i, m_2i) : i \in I_G\}$ of $\bar{M}$ is isomorphic to a direct product $G_1 \times R \times G_2$. Since $G$ is finite, the remark will follow from the fact that any subgroup $G = \{(m_1i, r_i, m_2i) : i \in I_G\}$ of $\bar{M}$ is isomorphic to a direct product $G_1 \times R \times G_2$. Since $G$ is finite, the remark will follow from the fact that any subgroup $G = \{(m_1i, r_i, m_2i) : i \in I_G\}$ of $\bar{M}$ is isomorphic to a direct product $G_1 \times R \times G_2$. Therefore it suffices to show that $N$ reduces to the neutral element $e' = (e_1, r, e_2)$ of $G$. To see this, let $g = (e_1, s, e_2)$ and $h = (e_1, t, e_2)$ be elements of $N$ inverse of each other. The relations $e' = e'^n, e' = gh$, and $g = e'ge'$ give, respectively, $r = e_2r \cup re_2, r = e_2t \cup se_2$, and $s = e_2r \cup e_2se_2 \cup re_2$. From the second and the first of these equations we get $e_2t \cup e_2se_2 = e_2r \subset r$. Thus, using the third equation, $s = r \cup e_2se_2$ where, as we have just seen, $e_2se_2 \subset r$. This gives $s = r$; hence $e' = g = h$, concluding the verification of the Remark.
and of $Q \subseteq Q'$ since $Q$ is defined as the least family to satisfy (K1) and (K2).

III. VERIFICATION OF $Q' \subseteq Q$

The family $Q'(1)$ consists of $X^*$ and of the empty set. Thus $Q'(1) \subseteq Q$ and it will suffice to consider an arbitrary fixed $\gamma \in \Gamma(n)$ and to show $\gamma^{-1}M' \subseteq Q$ for all $M' \subseteq M = \gamma X^*$ under the induction hypothesis $Q'(n-1) \subseteq Q$.

**Remark 3.** If $W_{M'} = \{m \in M : MmM \cap M' = \emptyset\}$ contains two elements or more, then $\gamma^{-1}M' \in Q$.

**Verification.** Let $\beta$ be a map of $M$ onto a set $\bar{M}$ that has the following two properties: $\beta$ sends $W_{M'}$ on a distinguished element $0$ of $\bar{M}$; the restriction of $\beta$ to $M \setminus W_{M'}$ is a bijection onto $\bar{M} \setminus \{0\}$.

Taking into account that, by definition, $W_{M'} = M \cdot W_{M'} \cdot M$, a structure of monoid is defined on $M$ by letting $(\beta m)(\beta m') = \beta(mm')$ for all $m, m' \in M$. Then, if $\operatorname{Card} W_{M'} \geq 2$, we have $\beta \gamma \in \Gamma(n-1)$ and, since $\gamma^{-1}M' = (\beta \gamma)^{-1}\beta M'$, the Remark is verified.

**Remark 4.** If $M'$ is an ideal (i.e., if $M' = M'M$ or $= MM'$), then $\gamma^{-1}M' \in Q$.

**Verification.** Because of left-right symmetry and of the finiteness of $M$, it suffices to consider the two cases of $M' = mM \neq MmM$ and of $M' = MmM = M$ where $m$ is an arbitrary fixed element of $M$.

Let $A = \gamma^{-1}(mM)$ (resp. $= \gamma^{-1}(MmM)$) and $B = A \setminus A \cdot X^* \cdot X^*$ (resp. $= A \setminus (X^* \cdot X \cdot A \cup A \cdot X \cdot X^* \cup X^* \cdot X \cdot A \cdot X \cdot X^*)$). By construction $B$ is the least subset of $X^*$ such that $A = B \cdot X^*$ (resp. $= X^* \cdot B \cdot X^*$) and the hypothesis $M' \neq M$ is equivalent to $e \notin B$. Further, let $M'' = \{m' \in M : \gamma^{-1}m' \cdot X \cap B \neq \emptyset\}$ (resp. $= \{m' \in M : \gamma^{-1}m' \cdot X \cap B \neq \emptyset\}$). Since $\gamma B \subseteq M' = M'M$ (resp. $= MM'M$) and $e \notin B$, we can find $X_0 \subseteq X$ and, for each $m' \in M''$, one subset $X_{m'}$ of $X$ (resp. two subsets $X_{m'}$ and $X_{m''}$ of $X$) in such a way that $A = X_0 \cdot X^* \cup \{\gamma^{-1}m' \cdot X_{m'} : m' \in M''\}$ (resp. $= X^* \cdot X_0 \cdot X^* \cup \{X^* \cdot X_{m'} \cdot X_{m''} \cdot X^* : m' \in M''\}$) and we have only to check $\operatorname{Card} W_{\{m\}} \geq 2$ for all $m' \in M''$.

First, let us recall the following consequence of Green (1951). If $P$ is a finite monoid and if $u, u' \in P$ satisfy $u' \in uP$ and either $u'P \neq uP$ or $Pu'P \neq PuP$, then $Pu'P \subseteq W_{\{u\}}$.

Indeed, assume $u' \in uP$ and $Pu'P \notin W_{\{u\}}$, that is, assume $u' = ua''$ and $u = au'a'$ for some $a, a', a'' \in P$. We have $u = a''u(a''a')^n$ for $n = 1$, hence for all $n \geq 1$. Since $P$ is finite there exist two positive integers $r$ and...
q such that $a^q = a^a a^q$. It follows that $u = a^u (a^a a^q)^q = a^a a^q - (a^a a^q)^q = a^u (a^a a^q)^q-1$ showing $u \in u' P$, i.e., $u P \subset u' P$. Since by hypothesis $u P \subset u P$ this gives the desired relations $u P = u P$ and $P u' P = P u P$.

(For later reference we note that if $P$ has only trivial subgroups, i.e., if $q = 1$, the same hypothesis give $u = a u$ hence $au' = au a^r = u a^r = u$ and, finally, $u = au a' = u a'$.)

Consider now $m' \in M^r$ and take $f \in \gamma^{-1} m'$ and $x \in X$ such that $fx \in B$ (resp. $x' fx \in B$ for some $x' \in X$). We have $\gamma fx = m' \gamma x \in m'M$ (resp. $\gamma fx \in m'M$ and $\gamma x'fx \in (\gamma x'M)^r$). Because of the minimal character of $B$, $\gamma fx \cdot M (= M' = M' \cdot M)$ is not equal to $m'M$ (resp. $\gamma x'fx \cdot M (= M' = M' \cdot M)$ is not equal to $M \cdot \gamma x'f \cdot M$, a fact which implies that, also, $\gamma fx \cdot M \neq m'M$). Thus $M' \cdot M' \cdot M \subset W_{m'}$ and $\text{Card } W_{m'} \geq 2$ because of the hypothesis $M' \neq M' \cdot M$ (resp $M' \cdot \gamma x'fx \cdot M \subset W_{m'}$ and $M \cdot \gamma x'fx \cdot M \subset W_{m'} \gamma x'f$, hence, using symmetry, $\gamma x'fx \cdot M \neq \gamma x'fx$).

Remark 5. For all $m \in M$, the set $(mM \cap Mm) \backslash W_{m}$ reduces to $\{m\}$.

Verification. The hypothesis $m' \in W_{m} \cap Mm$ is equivalent to the existence of $a, a', a'' \in M$ such that $m = ma'$; $m' = ma''$; $m' = m'a$. As mentioned above the first two relations imply $m = m'a$ and $m' = ma'$. Thus, by symmetry, $m = am'$ and $m' = ma'$ showing $m = m'$. This concludes the verification of Remark 5 and, in view of Remark 4, it also concludes the verification of $Q = Q'$.

IV. AN EXAMPLE OF EGGAN

Let $X = \{x_n\}_{n \in \mathbb{N}}$ and for each $k \in \mathbb{N}$ let $\lambda_k$ be the endomorphism of $X^*$ that sends each $x_n \in X$ onto $x_{n+2^k - 1}$ if $n < 2^k$ and $n = 0$, otherwise. Setting $B_1 = \{x_1\}$, we define inductively for $k > 1$, $B_k = B_{k-1} \cdot (x_{k-1})^* \cdot \lambda_k x_0$ where for any $A \subset X^*$, $A^*$ denotes the submonoid generated by $A$. In Eggan (1963), p. 389, it is shown that $B_k^*$ (denoted by $| \beta_k |$) has exactly star-height $k$.

It is clear that $B_1 \in Q$ and, to verify $B_{k+1} \in Q$, it suffices to verify $B_k^* \in Q$ under the induction hypothesis that $\gamma^{-1} \gamma B_k = B_k$ for some epimorphism $\gamma$ of $X^*$ onto a finite monoid having only trivial subgroups. Consider any element $f \in X^*.B_k$. Induction on the number of times $\lambda_k x_0$ appears in $f$ shows that either $f \in B_k^* \cdot B_k$ or $f \in V_k = \{f' \in X^* : f \cdot X^* \cap B_k^* = \emptyset\}$. Thus $B_k^* = \{e\} \cup X^* \cdot B_k \backslash V_k$ and since $V_k = \gamma^{-1} M'$ where $M' = \{m \in \gamma X^* : m \cdot \gamma X^* \cap \gamma B_k = \emptyset\}$ the result follows from the induction hypothesis.
It may not be too irrelevant to recall the following example which shows that sets of star-height one can have associated arbitrarily complex groups. Let \( x \) and \( y \) be two distinct elements of \( X \) and, for \( n > 3 \), let \( C_n = \{ x^n, x^{n-1}yx, x^{n-2}y, yx^{n-1} \} \cup \{ x^iyx^{n-i} : 1 \leq i \leq n - 3 \} \). Applying the theorem of Teissier (1951) shows that if \( \rho \) is a homomorphism of \( X^* \) into a finite monoid such that the sets \( \rho C_n^* \) and \( \rho C_n \cdot \rho x \) are disjoint, then \( \rho X^* \) contains at least one subgroup which admits the symmetric group \( S_n \) as a quotient group.

**Received:** March 20, 1964

**References**


McNaughton, R. (1960), Symbolic logic and automata. WADC Tech. Rept. 60-244.


